UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO

JESSE APTHORP, individually and on behalf of all others similarly situated, Plaintiff, v. HCF MANAGEMENT INC., and HCF OF CORRY, INC., doing business as CORRY MANOR, Defendants.	Case No. 3:25-cv-00085 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Jesse Apthorp ("Plaintiff"), individually, and on behalf of all others similarly situated, brings this action against HCF Management Inc., and HCF of Corry, Inc., doing business as Corry Manor (collectively, "HCF" or "Defendants"), by and through his attorneys, and allege, based upon personal knowledge as to his own actions, and based upon information and belief as to all other matters, as follows:

INTRODUCTION

1. HCF is a group of affiliated healthcare companies specializing in skilled nursing, rehabilitation, and assisted living facilities with more than two dozen locations across Ohio and Pennsylvania and headquartered in Lima, Ohio.[1]

2. As part of its operations HCF collects, maintains, and stores highly sensitive personal information belonging to its employees and patients, including, but not limited to: Social Security numbers, dates of birth, financial account numbers, medical information, and insurance information (collectively, "Private Information").

[1] *See generally* HCF Management, Inc., https://hcfinc.com/ (last accessed Jan. 15, 2025).

3. On October 3, 2024, HCF discovered suspicious activity on its computer network and prompted an internal investigation that determined on September 17, 2024, HCF suffered a Data Breach incident in which unauthorized cybercriminals accessed its information systems and databases and stole Private Information belonging to Plaintiff and Class members (the "Data Breach").

4. Starting on January 9, 2025, HCF sent notices to individuals whose information was accessed in the Data Breach.

5. Because HCF stored and handled such highly-sensitive Private Information, it had a duty and obligation to safeguard this information and prevent unauthorized third parties from accessing this data.

6. Ultimately, HCF failed to fulfill these obligations as unauthorized cybercriminals breached HCF's information systems and databases and stole vast quantities of Private Information belonging to Plaintiff and Class members. The Data Breach—and the successful exfiltration of Private Information—were the direct, proximate, and foreseeable results of multiple failings on the part of HCF.

7. The Data Breach occurred because HCF inexcusably failed to implement reasonable security protections to safeguard its information systems and databases. Prior to the Data Breach, HCF failed to inform the public that its data security practices were deficient and inadequate. Had Plaintiff and Class members been made aware of this fact, they would never have provided their Private Information to Defendants.

8. HCF's meager attempt to ameliorate the effects of this Data Breach with one year of complimentary credit monitoring is woefully inadequate. Much of this Private Information that

was stolen is immutable and one year of credit monitoring is nothing in the face of a life-long heightened risk of identity theft.

9. As a result of HCF's negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its contractual, statutory, and common-law obligations, Plaintiff and Class members suffered injuries as a result of HCF's conduct including, but not limited to:

- Lost or diminished value of their Private Information;
- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;
- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges;
- Time needed to change usernames and passwords on their accounts;
- Time needed to investigate, correct and resolve unauthorized access to their accounts; time needed to deal with spam messages and e-mails received subsequent to the Data Breach;
- Charges and fees associated with fraudulent charges on their accounts; and
- The continued and increased risk of compromise to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect their Private Information.

10. Accordingly, Plaintiff brings this action on behalf of all those similarly situated to seek relief for the consequences of Defendants' failure to reasonably safeguard Plaintiff's and Class members' Private Information; its failure to reasonably provide timely notification that Plaintiff's and Class members' Private Information had been compromised by an unauthorized third party; and for intentionally and unconscionably deceiving Plaintiff and Class members concerning the status, safety, location, access, and protection of their Private Information.

PARTIES

Plaintiff Jesse Apthorp

11. Plaintiff Jesse Apthorp is a resident and citizen of Corry, Pennsylvania. Plaintiff Apthorp was an employee of HCF from 2017-18 and received HCF's Data Breach Notice.

Defendant HCF Management, Inc.

12. Defendant HCF Management, Inc. is a corporation incorporated under the laws of the State of Ohio with its principal place of business at 1100 Shawnee Road, Lima, Ohio 458085.

Defendant HCF of Corry, Inc.

13. Defendant HCF of Corry, Inc. is a corporation incorporated under the laws of the State of Ohio with its principal place of business at 1100 Shawnee Road, Lima, Ohio 458085, which owns and does business under the fictitious name of Corry Manor in the State of Pennsylvania.

JURISDICTION AND VENUE

14. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, the number of class members exceeds 100, and at least one Class member is a citizen of a state different from HCF. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

15. This Court has personal jurisdiction over Defendants HCF Management, Inc., and HCF of Corry, Inc., because they are incorporated under the laws of the State of Ohio and have their principal places of business in this District, and because they regularly transact business in Ohio and have caused injury to residents of the State of Ohio.

16. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiff's and Class members' claims occurred in this District and because HCF resides in this District.

FACTUAL ALLEGATIONS

HCF – Background

17. HCF is a group of affiliated healthcare companies specializing in skilled nursing, rehabilitation, and assisted living facilities with more than two dozen locations across Ohio and Pennsylvania, and headquartered in Lima, Ohio.[2]

18. As part of its normal operations, Defendants collect, maintain, and store the highly sensitive Private Information provided by its current and former employees and patients, including but not limited to: Social Security numbers, dates of birth, financial account numbers, medical information, and insurance information.

19. Current and former employees and patients of Defendants made their Private Information available to HCF with the reasonable expectation that any entity with access to this information would keep that sensitive and personal information confidential and secure from illegal and unauthorized access. They similarly expected that, in the event of any unauthorized access, these entities would provide them with prompt and accurate notice.

20. This expectation was objectively reasonable and based on an obligation imposed on HCF by statute, regulations, industrial custom, and standards of general due care.

21. Unfortunately for Plaintiff and Class members, HCF failed to carry out its duty to safeguard sensitive Private Information and provide adequate data security. As a result, it failed to

[2] *Id.*

protect Plaintiff and Class members from having their Private Information accessed and stolen during the Data Breach.

The Data Breach

22. According to information provided by HCF, cybercriminals breached HCF's information systems and databases on September 17, 2024. On November 19, 2024—two months after the Data Breach—HCF's investigation with cybersecurity experts confirmed Private Information was exfiltrated from its network in the Data Breach.

23. Starting on January 9, 2025, HCF sent notice of the Data Breach to all individuals affected by this data security incident.

24. Omitted from the notice were the date that Defendants detected the Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

25. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

26. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiff and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

27. The attacker accessed and acquired files in Defendants' computer systems containing unencrypted Private Information of Plaintiff and Class Members, including their names, addresses, dates of birth, Social Security numbers, PHI, and other sensitive information. Plaintiff's and Class Members' Private Information was accessed and stolen in the Data Breach.

28. Plaintiff further believes that the Private Information and that of Class Members was or will be sold on the dark web, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

HCF's Many Failures Both Prior to and Following the Breach

29. Defendants collect and maintain vast quantities of Private Information belonging to Plaintiff and Class members as part of its normal operations. The Data Breach occurred as direct, proximate, and foreseeable results of multiple failings on the part of Defendants.

30. First, Defendants failed to implement reasonable security protections to safeguard its information systems and databases.

31. Second, Defendants failed to inform the public that its data security practices were deficient and inadequate. Had Plaintiff and Class members been aware that Defendants did not have adequate safeguards in place to protect such sensitive Private Information, they would never have provided such information to Defendants.

32. Additionally, Defendants' attempt to ameliorate the effects of this Data Breach with one year of complimentary credit monitoring is woefully inadequate. Plaintiff's and Class members' Private Information was accessed and acquired by cybercriminals for the express purpose of misusing the data. As a consequence, they face the real, immediate, and likely danger of identity theft and misuse of their Private Information. And this can, and in some circumstances already has, caused irreparable harm to their personal, financial, reputational, and future well-

being. This harm is even more acute because much of the stolen Private Information, such as a Social Security number, is immutable.

33. In short, Defendants' myriad failures, including the failure to timely notify Plaintiff and Class members that their personal information had been stolen due to Defendants' security failures, allowed unauthorized individuals to access, misappropriate, and misuse Plaintiff's and Class members' Private Information for more than sixty (60) days before Defendants finally granted victims the opportunity to take proactive steps to defend themselves and mitigate the near- and long-term consequences of the Data Breach.

Data Breaches Pose Significant Threats

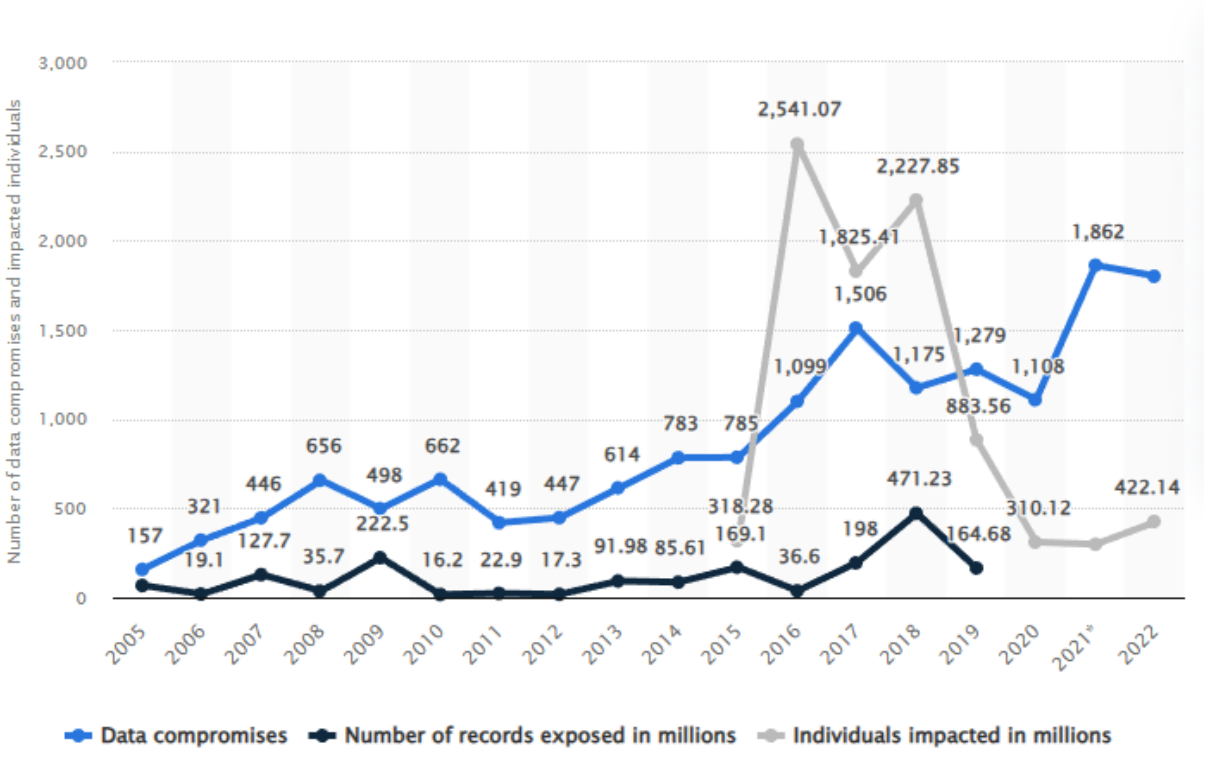
34. Data Breaches have become a constant threat that, without adequate safeguards, can expose personal data to malicious actors. It is well known that Private Information, Social Security numbers in particular, is an invaluable commodity and a frequent target of hackers.

35. In 2022, the Identity Theft Resource Center's Annual End-of-Year Data Breach Report listed 1,802 total compromises involving 422,143,312 victims for 2022, which was just 50 compromises short of the current record set in 2021.[3] The HIPAA Journal's 2022 Healthcare Data Breach Report reported 707 compromises involving healthcare data, which is just 8 shy of the record of 715 set in 2021 and still double that of the number of similar such compromises in 2017 and triple the number of compromises in 2012.[4]

[3] Identity Theft Resource Center, *2022 End of Year Data Breach Report* (Jan. 25, 2023), https://www.idtheftcenter.org/publication/2022-data-breach-report/?utm_source=press+release&utm_medium=web&utm_campaign=2022+Data+Breach+Report (last visited Jan. 16, 2025).

[4] Rebecca Murray-Watson, *2022 Healthcare Data Breach Report*, The HIPAA Journal (Jan. 24, 2023), https://www.hipaajournal.com/2022-healthcare-data-breach-report/ (last visited Jan. 16, 2025).

36. Statista, a German entity that collects and markets data relating to, among other things, Data Breach incidents and the consequences thereof, confirms that the number of Data Breaches has been steadily increasing since it began a survey of data compromises in 2005 with 157 compromises reported that year, to a peak of 1,862 in 2021, to 2022's total of 1,802.[5] The number of impacted individuals has also risen precipitously from approximately 318 million in 2015 to 422 million in 2022, which is an increase of nearly 50%.[6]



[5] Statista, *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2022* (2025), https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (last visited Jan. 16, 2025).

[6] *Id.*

37. This stolen Private Information is then routinely traded on dark web black markets as s simple commodity, with social security numbers being so ubiquitous to be sold at as little as $2.99 apiece and passports retailing for as little as $15 apiece.[7]

38. In addition, the severity of the consequences of a compromised social security number belies the ubiquity of stolen numbers on the dark web. Criminals and other unsavory elements can fraudulently take out loans under the victims' name, open new lines of credit, and cause other serious financial difficulties for victims:

> Scammers use your Social Security number (SSN) to get other personal information about you. They can use your SSN and your good credit to apply for more credit in your name. Then, when they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your SSN until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought.[8]

39. This is exacerbated by the fact that the problems arising from a compromised social security number are exceedingly difficult to resolve. A victim is forbidden from proactively changing his or her number unless and until it is actually misused and harm has already occurred. And even this delayed remedial action is unlikely to undo the damage already done to the victims:

> You should know that other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So, using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> . . . .

---

[7] Edvardas Mikalauskas, *What is your identity worth on the dark web?*, Cybernews (Sept. 28, 2021), https://cybernews.com/security/whats-your-identity-worth-on-dark-web/ (last visited Jan. 16, 2025).

[8] U.S. Soc. Security Admin., *Identity Theft and Your Social Security Number*, at 1 (Oct. 2024), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 16, 2025).

> For some victims of identity theft, a new number actually creates new problems. If the old credit information isn't associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit.[9]

40. The most sought after and expensive information on the dark web are stolen medical records which command prices from $250 to $1,000 each.[10] Medical records are considered the most valuable because unlike credit cards, which can easily be canceled, and Social Security numbers, which can be changed, medical records contain "a treasure trove of unalterable data points, such as a patient's medical and behavioral health history and demographics, as well as their health insurance and contact information."[11] With this bounty of ill-gotten information, cybercriminals can steal victims' public and insurance benefits and bill medical charges to victims' accounts.[12] Cybercriminals can also change the victims' medical records, which can lead to misdiagnosis or mistreatment when the victims seek medical treatment.[13] Victims of medical identity theft could even face prosecution for drug offenses when cybercriminals use their stolen information to purchase prescriptions for sale in the drug trade.[14]

---

[9] *Id.* at 6.

[10] Paul Nadrag, *Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web*, Fierce Healthcare (Jan. 26, 2021), https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web (last visited Jan. 16, 2025).

[11] *Id.*

[12] Identity Theft Guard Solutions, Inc., *Medical Identity Theft in the New Age of Virtual Healthcare*, IDX (March 15, 2021), https://www.idx.us/knowledge-center/medical-identity-theft-in-the-new-age-of-virtual-healthcare (last visited Jan. 16, 2025). *See also* Michelle Andrews, *The Rise of Medical Identity Theft*, Consumer Reports (Aug. 25, 2016), https://www.consumerreports.org/health/medical-identity-theft-a1699327549/ (last visited Jan. 16, 2025).

[13] *Id.*

[14] *Id.*

41. The wrongful use of compromised medical information is known as medical identity theft and the damage resulting from medical identity theft is routinely far more serious than the harm resulting from the theft of simple PII. Victims of medical identity theft spend an average of $13,500 to resolve problems arising from medical identity theft and there are currently no laws limiting a consumer's liability for fraudulent medical debt (in contrast, a consumer's liability for fraudulent credit card charges is capped at $50).[15] It is also "considerably harder" to reverse the damage from the aforementioned consequences of medical identity theft.[16]

42. Instances of Medical identity theft have grown exponentially over the years from approximately 6,800 cases in 2017 to just shy of 43,000 in 2021, which represents a seven-fold increase in the crime.[17]

43. In light of the dozens of high-profile health and medical information data breaches that have been reported in recent years, entities like Defendants charged with maintaining and securing patient PII should know the importance of protecting that information from unauthorized disclosure. Indeed, Defendants knew, or certainly should have known, of the recent and high-profile data breaches in the health care industry: UnityPoint Health, Lifetime Healthcare, Inc., Community Health Systems, Kalispell Regional Healthcare, Anthem, Premera Blue Cross, and many others.[18]

44. In addition, the Federal Trade Commission ("FTC") has brought dozens of cases against companies that have engaged in unfair or deceptive practices involving inadequate

[15] AARP, Medical Identity Theft (Mar. 25, 2022), https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html (last visited Jan. 16, 2025).

[16] *Id.*

[17] *Id.*

[18] *See, e.g.*, Steve Alder, *Healthcare Data Breach Statistics*, HIPAA Journal (Jan. 15, 2025), https://www.hipaajournal.com/healthcare-data-breach-statistics (last visited Jan. 16, 2025).

protection of consumers' personal data, including recent cases against LabMD, Inc., SkyMed International, Inc., and others. The FTC publicized these enforcement actions to place companies like Defendants on notice of their obligation to safeguard customer and patient information.[19]

45. Given the nature of Defendants' Data Breach, as well as the length of the time Defendants' networks were breached and the long delay in notification to the Class, it is foreseeable that the compromised Private Information has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff's and Class members' Private Information can easily obtain Plaintiff's and Class members' tax returns or open fraudulent credit card accounts in Class members' names.

46. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer Data Breach, because credit card victims can cancel or close credit and debit card accounts.[20] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

47. To date, Defendants have offered its consumers only 12 months of identity theft monitoring services. The offered services are inadequate to protect Plaintiff and the Class from the

[19] *See e.g.*, Decision and Order, *In the Matter of SKYMED INTERNATIONAL, INC.*, No. C-4732 (F.T.C. Jan. 26, 2021), https://www.ftc.gov/system/files/documents/cases/c-4732_skymed_final_order.pdf (last visited Jan. 16, 2025).

[20] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes (Mar 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last visited Jan. 16, 2025). *See also* Identity Theft Resource Center, *Why Your Social Security Number Isn't as Valuable as Your Login Credentials* (June 18, 2021), https://www.idtheftcenter.org/post/why-your-social-security-number-isnt-as-valuable-as-your-login-credentials/ (last visited Jan. 16, 2025).

threats they will face for years to come, particularly in light of the Private Information at issue here.

48. Despite the prevalence of public announcements of Data Breach and data security compromises, its own acknowledgment of the risks posed by Data Breaches, and its own acknowledgment of its duties to keep Private Information private and secure, Defendants failed to take appropriate steps to protect the Private Information of Plaintiff and the Class from misappropriation. As a result, the injuries to Plaintiff and the Class were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for its current and former employees and patients.

Defendants Failed to Comply with HIPAA

49. Defendants are covered entities or business associate under HIPAA (45 C.F.R. § 160.103) and are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

50. Defendants are subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[21] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

51. "Electronic protected health information," which is protected under state and federal law, is defined as "individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

[21] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

52. Guidance from the United States Department of Health and Human Services ("HHS") instructs healthcare providers that even patient status alone is protected by HIPAA. In *Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule*, HHS instructs:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such Information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data . . . . If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[22]

53. HIPAA's Security Rule requires Defendants to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

54. HIPAA also requires Defendants to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendants are

[22] U.S. Dept. of Health & Human Servs., *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, (Nov. 26, 2012), https://www.hhs.gov/hipaa/for-professionals/special-topics/de-identification/index.html (last visited Jan. 16, 2025).

required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

55. HIPAA and HITECH also obligated Defendants to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

56. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendants to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[23]

57. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

58. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

[23] *See* U.S. Dept. of Health & Human Servs., *Breach Notification Rule* (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added) (last visited Jan. 16, 2025).

59. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule."[24] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI."[25]

Ohio Law is Consistent with HIPAA

60. Ohio has made its laws governing the use and disclosure of protected health information consistent with HIPAA. *See* R.C. 3798.01, *et seq.* Ohio law adopts the same definitions of "covered entity," "disclosure," "health care provider," "health information," "protected health information," "individually identifiable health information," and "use" as provided by the HIPAA Privacy Rule. *See* R.C. 3798.01. Furthermore, it was "the intent of the general assembly in enacting [R.C. 3798.01 et seq.] to make the laws of [Ohio] governing the use and disclosure of protected health information by covered entities consistent with, but generally not more stringent than, the HIPAA privacy rule for the purpose of eliminating barriers to the adoption and use of electronic health records and health information exchanges." R.C. 3798.02.

[24] U.S. Dept. of Health & Human Servs., *Security Rule Guidance Material* (Oct. 24, 2024), http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last visited Jan. 16, 2025).

[25] U.S. Dept. of Health & Human Servs., *Guidance on Risk Analysis* (July 22, 2019), http://hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last visited Jan. 16, 2025).

61. Under R.C. 3798.03(A)(2), Defendants were required to "[i]mplement and maintain appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information in a manner consistent with 45 C.F.R. 164.530(c)."

62. Under R.C. 3798.04, Defendants are not permitted to:

(A) Use or disclose protected health information without an authorization that is valid under 45 C.F.R. 164.508 and, if applicable, 42 C.F.R. part 2, except when the use or disclosure is required or permitted without such authorization by Subchapter C of Subtitle A of Title 45 of the Code of Federal Regulations and, if applicable, 42 C.F.R. part 2;

(B) Use or disclose protected health information in a manner that is not consistent with 45 C.F.R. 164.502.

63. Because Ohio law expressly incorporates the standards set forth by HIPAA and its regulations, Defendant's violations of HIPAA constitute a violation of Ohio law.

FTC Act Requirements and Violations

64. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

65. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and

practices for business.[26] The guidelines note businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.[27] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[28] Defendants clearly failed to do any of the foregoing, as evidenced by the length of the Data Breach, the fact that the Breach went undetected, and the amount of data exfiltrated.

66. The FTC further recommends that companies not maintain personally identifying information longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

67. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

---

[26] FTC, *Protecting Personal Information: A Guide for Business* (October 2016), https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last visited Jan. 16, 2025).

[27] *Id.*

[28] *Id.*

68. As evidenced by the Data Breach, Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

69. Defendants were fully aware of its obligation to protect the Private Information of its current and former employees and patients, including Plaintiff and the Class, and on information and belief, Defendants are a sophisticated and technologically savvy entities that relies extensively on technology systems and networks to maintain their practice, including storing employees and patients' Private Information in order to operate the business.

70. Defendants had and continues to have a duty to exercise reasonable care in collecting, storing, and protecting the Private Information from the foreseeable risk of a Data Breach. The duty arises out of the special relationship that exists between Defendants and Plaintiff and Class members. Defendants alone had the exclusive ability to implement adequate security measures to its cyber security network to secure and protect Plaintiff's and Class members' Private Information.

Industry Standards and Noncompliance

71. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

72. Some industry best practices that should be implemented by businesses dealing with sensitive Private Information like Defendants include but are not limited to: educating all employees and patients, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and

limiting which employees and patients can access sensitive data. As evidenced by the Data Breach, Defendants failed to follow some or all of these industry best practices.

73. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendants failed to follow these cybersecurity best practices.

74. Defendants should have also followed the minimum standards of any one of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

75. Defendants failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

Plaintiff and the Class Suffered Harm Resulting from the Data Breach

76. Like any data hack, the Data Breach presents major problems for all affected.[29]

77. The FTC warns the public to pay particular attention to how they keep personally identifying information including Social Security numbers and other sensitive data. As the FTC notes, "once identity thieves have your personal information, they can drain your bank account,

[29] Paige Schaffer, *Data Breaches' Impact on Consumers*, Insurance Thought Leadership (July 29, 2021), https://www.insurancethoughtleadership.com/cyber/data-breaches-impact-consumers (last visited Jan. 16, 2025).

run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[30]

78. The ramifications of Defendants' failure to properly secure Plaintiff's and Class members' Private Information are severe. Identity theft occurs when someone uses another person's financial, and personal information, such as that person's name, address, Social Security number, and other information, without permission in order to commit fraud or other crimes.

79. According to data security experts, one out of every four Data Breach notification recipients become a victim of identity fraud.

80. Furthermore, Private Information has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.

81. Accordingly, Defendants' wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the Class at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. According to a recent study published in the scholarly journal "Preventive Medicine Reports", public and corporate Data Breaches correlate to an increased risk of identity theft for victimized consumers.[31] The same study also found that identity theft is a deeply traumatic event for the victims, with more than a quarter of victims still experiencing sleep problems, anxiety, and irritation even six months after the crime.[32]

---

[30] *FTC, Warning Signs of Identity Theft* (undated), https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft (last visited Jan. 16, 2025).

[31] David Burnes, Marguerite DeLiema, Lynn Langton, *Risk and protective factors of identity theft victimization in the United States*, 17 Preventive Medicine Reports 101058 (Jan. 23, 2020), https://www.sciencedirect.com/science/article/pii/S2211335520300188?via%3Dihub (last visited Jan. 16, 2025).

[32] *Id.*

82. There is also a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that has not yet been exploited by cybercriminals presents a concrete risk that the cybercriminals who now possess Class members' Private Information will do so at a later date or re-sell it.

83. Data Breaches have also proven to be costly for affected organizations as well, with the average cost to resolve being $4.88 million dollars in 2024.[33]

84. The theft of medical information, beyond the theft of more traditional forms off PII, is especially harmful for victims. Medical identity theft, the misuse of stolen medical records and information, has seen a seven-fold increase over the last five years and this explosive growth far outstrips the increase in incidence of traditional identity theft.[34] Medical Identity Theft is especially nasty for victims because of the lack of laws that limit a victim's liabilities and damages from this type of identity theft (e.g., a victim's liability for fraudulent credit card charges is capped at $50), the unalterable nature of medical information, the sheer costs involved in resolving the fallout from a medical identity theft (victims spend, on average, $13,500 to resolve problems arising from this crime), and the risk of criminal prosecution under anti-drug laws.[35]

85. In response to the Data Breach, Defendants offered to provide certain individuals whose Private Information was exposed in the Data Breach with just 12 months of credit monitoring through Identity Defense. However, this is much shorter than what is necessary to protect against the lifelong risk of harm imposed on Plaintiff and Class members by Defendants' failures.

---

[33] IBM Security, *Cost of a Data Breach Report 2024*, https://www.ibm.com/reports/data-breach (last visited Jan. 16, 2025).

[34] AARP, *supra*, https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html.

[35] *Id.*

86. Moreover, the credit monitoring offered by Defendants is fundamentally inadequate to protect them from the injuries resulting from the unauthorized access and exfiltration of their sensitive Private Information.

87. Here, due to the Breach, Plaintiff and Class members have been exposed to injuries that include, but are not limited to:

a. Theft of Private Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts as a direct and proximate result of the Private Information stolen during the Data Breach;

c. Damages arising from the inability to use accounts that may have been compromised during the Data Breach;

d. Costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach, such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, placing freezes and alerts on their credit reports, contacting their financial institutions to notify them that their personal information was exposed and to dispute fraudulent charges, imposition of withdrawal and purchase limits on compromised accounts, including but not limited to lost productivity and opportunities, time taken from the enjoyment of one's life, and the inconvenience, nuisance, and annoyance of dealing with all issues resulting from the Data Breach, if they were fortunate enough to learn of the Data Breach despite Defendants' delay in disseminating notice in accordance with state law;

e. The imminent and impending injury resulting from potential fraud and identity theft posed because their Private Information is exposed for theft and sale on the dark web; and

f. The loss of Plaintiff's and Class members' privacy.

88. Plaintiff and Class members have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their Private Information being accessed by cybercriminals, risks that will not abate within a mere 12 months: the unauthorized access of Plaintiff's and Class members' Private Information, especially their

Social Security numbers, puts Plaintiff and the Class at risk of identity theft indefinitely, and well beyond the limited period of credit monitoring that Defendants offered victims of the Breach.

89. As a direct and proximate result of Defendants' acts and omissions in failing to protect and secure Private Information, Plaintiff and Class members have been placed at a substantial risk of harm in the form of identity theft, and have incurred and will incur actual damages in an attempt to prevent identity theft.

90. Plaintiff retains an interest in ensuring there are no future breaches, in addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of both himself and similarly situated individuals whose Private Information was accessed in the Data Breach.

PLAINTIFF'S EXPERIENCES

Plaintiff Apthorp

91. Plaintiff Jesse Apthorp was an employee of HCF from 2017-2018.

92. As a condition of his employment, Plaintiff Apthorp was required to provide his Private Information to Defendants.

93. Plaintiff Apthorp received HCF's data breach notice. The notice informed Plaintiff Apthorp that his Private Information was improperly accessed and obtained by third parties.

94. After the breach, Plaintiff Apthorp experienced a dramatic increase in the number of spam phone calls, text messages, and emails.

95. Further, Plaintiff Apthorp suffered a fraudulent auto loan report on his credit stating he owed $70,000 on a vehicle he does not own.

96. As a result of the Data Breach and the resulting suspicious activity, Plaintiff Apthorp made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. He has also spent

several hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including, but not limited to, work and recreation.

97. As a result of the Data Breach, Plaintiff Apthorp suffered anxiety due to the public dissemination of his personal information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using his private information for purposes of identity theft and fraud. Plaintiff Apthorp is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

98. Plaintiff Apthorp suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendants obtained from him; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

99. As a result of the Data Breach, Plaintiff Apthorp anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. And, as a result of the Data Breach, he is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

CLASS REPRESENTATION ALLEGATIONS

100. Plaintiff brings this action on behalf of himself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a Class of:

> **All persons in the United States whose Private Information was accessed in the Data Breach.**

Excluded from the Class are Defendants, their executives and officers, and the Judge(s) assigned to this case. Plaintiff reserves the right to modify, change or expand the Class definition after conducting discovery.

101. Numerosity: Upon information and belief, the Class is so numerous that joinder of all members is impracticable with an estimated tens of thousands of affected individuals. The exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of Defendants and obtainable by Plaintiff only through the discovery process. The members of the Class will be identifiable through information and records in Defendants' possession, custody, and control.

102. Existence and Predominance of Common Questions of Fact and Law: Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

a. When Defendants learned of the Data Breach;

b. Whether hackers obtained Class members' Private Information via the Data Breach;

c. Whether Defendants' response to the Data Breach was adequate;

d. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

e. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations, industry standards, and/or its own promises and representations;

f. Whether Defendants knew or should have known that its data security systems and monitoring processes were deficient;

g. Whether Defendants owed a duty to Class members to safeguard their Private Information;

h. Whether Defendants breached the duty to Class members to safeguard their Private Information;

i. Whether Defendants had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class members;

j. Whether Defendants breached the duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class members;

k. Whether Defendants' conduct violated the FTCA, HIPAA and/or the Consumer Protection Act invoked herein;

l. Whether Defendants' conduct was negligent;

m. Whether Defendants' conduct was *per se* negligent;

n. Whether Defendants were unjustly enriched;

o. What damages Plaintiff and Class members suffered as a result of Defendants' misconduct;

p. Whether Plaintiff and Class members are entitled to actual damages;

q. Whether Plaintiff and Class members are entitled to additional credit or identity monitoring and monetary relief; and

r. Whether Plaintiff and Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

103. Typicality: All of Plaintiff's claims are typical of the claims of the Class since Plaintiff and all members of the Class had their Private Information compromised in the Data Breach. Plaintiff's claims and damages are also typical of the Class because they resulted from Defendants' uniform wrongful conduct. Likewise, the relief to which Plaintiff is entitled to is typical of the Class because Defendants have acted, and refused to act, on grounds generally applicable to the Class.

104. Adequacy: Plaintiff is an adequate class representative because Plaintiff's interests do not materially or irreconcilably conflict with the interests of the Class Plaintiff seeks to

represent, Plaintiff retained counsel competent and highly experienced in complex class action litigation, and intend to prosecute his action vigorously. Plaintiff and his counsel will fairly and adequately protect the interests of the Class. Neither Plaintiff nor his counsel has any interests that are antagonistic to the interests of other members of the Class.

105. Superiority: Compared to all other available means of fair and efficient adjudication of the claims of Plaintiff and the Class, a class action is the most superior. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendants' conduct. It would be virtually impossible for members of the Class individually to effectively redress the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Members of the Class can be readily identified and notified based on, *inter alia*, Defendants' records and databases.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On behalf of Plaintiff and the Class)

106. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

107. Defendants owe a duty of care to protect the Private Information belonging to Plaintiff and Class members. Defendants also owe several specific duties including, but not limited

to, the duty:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. to protect employees and patients' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. to have procedures in place to detect the loss or unauthorized dissemination of Private Information in its possession;

d. to implement processes to quickly detect a Data Breach and to timely act on warnings about Data Breaches; and

e. to promptly notify Plaintiff and Class members of the Data Breach, and to precisely disclose the type(s) of information compromised.

108. Defendants also owe them a duty because Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, as well as analogous state statutes like Ohio Revised Code § 1345.01, *et seq.*, require Defendants to use reasonable measures to protect confidential data.

109. Defendants also owe them duty because industry standards mandate that Defendants protect their employees' and patients' confidential Private Information.

110. Defendants also owe a duty because it had a special relationship with Plaintiff's and Class members. Plaintiff and Class members entrusted their Private Information to Defendants on the understanding that adequate security precautions would be taken to protect their information. Furthermore, only Defendants had the ability to protect its systems and the Private Information stored on them from attack.

111. Defendants also owe a duty to timely disclose any unauthorized access and/or theft of the Private Information belonging to Plaintiff and the Class. Their duty exists to allow Plaintiff and the Class the opportunity to undertake appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Private Information.

112. Defendants breached the duties to Plaintiff and the Class by failing to take reasonable appropriate measures to secure, protect, and/or otherwise safeguard the Private Information belonging to Plaintiff and Class members.

113. Defendants also breached the duties owed to Plaintiff and the Class by failing to timely and accurately disclose to Plaintiff and Class members that their Private Information had been improperly acquired and/or accessed.

114. As a direct and proximate result of Defendants' negligent or reckless conduct, Plaintiff and the Class were injured in the ways described above.

115. Plaintiff and Class members were foreseeable victims of any inadequate security practices on the part of Defendants and the injuries (and resulting damages) they suffered were the foreseeable result of the aforementioned inadequate security practices.

116. In failing to provide prompt and adequate individual notice of the Data Breach, Defendants also acted with reckless disregard for the rights of Plaintiff and Class members.

117. Plaintiff is entitled to nominal and/or compensatory damages in an amount to be proven at trial and injunctive relief requiring Defendants to, *inter alia*, strengthen the data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class members.

COUNT II
NEGLIGENCE *PER SE*
(On behalf of Plaintiff and the Class)

118. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

119. Section 5 of the FTCA and analogous state statutes (like Ohio Revised Code § 1345.01, *et seq.*) impose a duty on Defendants to provide fair and adequate data security to secure, protect, and/or otherwise safeguard the Private Information of Plaintiff and Class members.

120. Defendants violated the FTCA, as well as analogous state statutes and regulations, by failing to provide fair, reasonable, or adequate computer systems and data security practices to secure, protect, and/or otherwise safeguard Plaintiff's and Class members' Private Information.

121. Defendants' failure to comply with the FTCA and similar state law constitutes negligence *per se*.

122. Plaintiff and Class members are within the class of persons that the FTCA and analogous state laws are intended to protect.

123. It was reasonably foreseeable that the failure to protect and secure Plaintiff's and Class members' Private Information in compliance with applicable laws and industry standards would result in that Information being accessed and stolen by unauthorized actors.

124. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, the injuries described above.

125. Plaintiff and Class members are entitled to nominal and/or compensatory damages in an amount to be proven at trial and injunctive relief requiring Defendants to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class members.

COUNT III
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Class)

126. Plaintiff incorporates and realleges all allegations above as if fully set forth herein, with the exception that this claim is brought in the alternative to the claims for negligence and negligence *per se*.

127. Plaintiff and the Class provided Defendants with their Private Information.

128. By providing their Private Information, and upon Defendants' acceptance of their information, Plaintiff and the Class, on one hand, and Defendants, on the other hand, entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contract entered into between the parties.

129. The implied contracts between Defendants and Plaintiff and Class members obligated Defendants to take reasonable steps to secure, protect, safeguard, and keep confidential Plaintiff's and Class members' Private Information. The terms of these implied contracts are described in federal laws, state laws, and industry standards, as alleged above. Defendants expressly adopted and assented to these terms in its public statements, representations and promises as described above.

130. The implied contracts for data security also obligated Defendants to provide Plaintiff and Class members with prompt, timely, and sufficient notice of any and all unauthorized access or theft of their Private Information.

131. Defendants breached these implied contracts by failing to take, develop and implement adequate policies and procedures to safeguard, protect, and secure the Private Information belonging to Plaintiff and Class members; allowing unauthorized persons to access Plaintiff's and Class members' Private Information; and failing to provide prompt, timely, and sufficient notice of the Data Breach to Plaintiff and Class members, as alleged above.

132. As a direct and proximate result of Defendants' breaches of the implied contracts, Plaintiff and the Class have been damaged as described herein, will continue to suffer injuries as detailed above due to the continued risk of exposure of Private Information, and are entitled to damages in an amount to be proven at trial.

COUNT IV
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Class)

133. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

134. This count is brought in the alternative to Count III.

135. Plaintiff and the Class have a legal and equitable interest in their Private Information that was collected and maintained by Defendants.

136. Defendants were benefitted by the conferral upon them of Plaintiff's and Class members' Private Information and by their ability to retain and use that information. Defendants understood that they were in fact so benefitted.

137. Defendants also understood and appreciated that Plaintiff's and Class members' Private Information was private and confidential and its value depended upon Defendants maintaining the privacy and confidentiality of that information.

138. But for Defendants' willingness and commitment to maintain their privacy and confidentiality, Plaintiff and Class members would not have provided or authorized their Private Information to be provided to Defendants, and Defendants would have been deprived of the competitive and economic advantages it enjoyed by falsely claiming that its data-security safeguards met reasonable standards. These competitive and economic advantages include, without limitation, wrongfully gaining students, gaining the reputational advantages conferred upon it by Plaintiff and Class members, collecting excessive advertising and sales revenues as described herein, monetary savings resulting from failure to reasonably upgrade and maintain data technology infrastructures, staffing, and expertise raising investment capital as described herein, and realizing excessive profits.

139. As a result of Defendants' wrongful conduct as alleged herein (including, among other things, its deception of Plaintiff, the Class, and the public relating to the nature and scope of the data breach; its failure to employ adequate data security measures; its continued maintenance and use of the Private Information belonging to Plaintiff and Class members without having adequate data security measures; and its other conduct facilitating the theft of that Private Information), Defendants have been unjustly enriched at the expense of, and to the detriment of, Plaintiff and the Class.

140. Defendants' unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and Class members' sensitive Private Information, while at the same time failing to maintain that information secure from intrusion.

141. Under the equitable doctrine of unjust enrichment, it is inequitable for Defendants to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiff and the Class in an unfair and unconscionable manner. Defendants' retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

142. The benefit conferred upon, received, and enjoyed by Defendants was not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendants to retain the benefit.

143. Defendants are therefore liable to Plaintiff and the Class for restitution in the amount of the benefit conferred on Defendants as a result of its wrongful conduct, including specifically the value to Defendants of the PII that was accessed in the Data Breach and the profits Defendants receives from the use and sale of that information.

144. Plaintiff and Class members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from its wrongful conduct.

145. Plaintiff and Class members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT V
BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiff and the Class)

146. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

147. Defendants had a fiduciary duty to adequately safeguard its patients' Private Information and keep it confidential. Such information may not be disclosed to any party without consent. Furthermore, should PHI be disclosed without consent, Defendants have a fiduciary duty to provide timely notification.

148. Defendants breached their fiduciary duty to Plaintiff and Class Members by failing to adequately protect against cybersecurity events and give notice of the Data Breach in a reasonable and practicable period of time.

149. Defendants' fiduciary duties and violations thereof are informed by HIPAA and analogous state law.

150. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic PHI Defendants created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

151. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to implement technical policies and procedures for electronic information systems that

maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1).

152. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1).

153. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii).

154. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2).

155. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3).

156. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(94).

157. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.

158. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5).

159. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

160. Defendants breached their fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

161. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, as described above. Accordingly, Plaintiff and Class Members are entitled to compensatory, consequential, and/or nominal damages in an amount to be determined.

162. Defendant's breaches of fiduciary duty are ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and insecure manner. Moreover, Defendants continue to withhold material information about the Data Breach from their patients.

163. Plaintiff and Class Members are entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; (iii) continue to provide adequate credit monitoring to all Class Members; and (iv) provide complete and accurate information to its patients about the Data Breach and the risk its patients face.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all members of the Class, respectfully requests that the Court enter judgment in his favor and against Defendants, as follows:

A. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is a proper class representative; and appoint Plaintiff's Counsel as Class Counsel;

B. That the Court award Plaintiff and Class members nominal, compensatory, consequential, and general damages in an amount to be determined at trial;

C. That the Court award Plaintiff and Class members statutory damages, and punitive or exemplary damages, to the extent permitted by law;

D. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

E. That the Court award pre- and post-judgment interest at the maximum legal rate;

F. That the Court award grant all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution; and

G. That the Court grant all other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the putative Class, hereby demands a trial by jury of all issues so triable.

Date: January 16, 2025

Respectfully submitted,

/s/ *Terence R. Coates*

Terence R. Coates (0085579)
Dylan J. Gould (0097954)
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, Ohio 45202

Telephone: (513) 651-3700
Facsimile: (513) 665-0219
tcoates@msdlegal.com
dgould@msdlegal.com

Daniel O. Herrera*
Nickolas J. Hagman*
Mohammed A. Rathur*
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com
mrathur@caffertyclobes.com

* *Pro Hac Vice* forthcoming

Attorneys for Plaintiff and the Proposed Class